CONTINUATION OF APPLICATION FOR SEARCH WARRANT

I, James Walsh, a Special Agent of the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF"), being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am submitting this continuation in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a digital device currently in law-enforcement possession and described in Attachment A, and the extraction from that property of electronically-stored information as described in Attachment B.

2. I am a Special Agent with ATF, and have been since 1998. My responsibilities include investigating criminal violations of Titles 18 and 21 of the United States Code. I have participated in hundreds of investigations involving firearms and narcotics, many of which have resulted in the arrest and conviction of criminal defendants and the seizure of firearms and narcotics. From 1992 to 1998, I was a Special Agent with the U.S. Secret Service, and in that role I conducted numerous investigations involving counterfeit U.S. currency. The matters set forth in this continuation are either known personally to me or were related to me by other persons acting in their official capacities as officers and agents of the United States, the State of Michigan, and local jurisdictions within Michigan.

3. Because it is submitted for the limited purpose of establishing probable cause to search for evidence, this affidavit does not necessarily recite all of the facts of the underlying investigation that are known to me or to other investigators at this time. I submit that the matters set forth in this continuation demonstrate probable cause to believe that property (defined in Fed. R. Crim. P. 41(a)(2)(A) as including information) as described in Attachment "B" to the Search Warrant Application will be found at the place to be searched, and that those items constitute evidence of the following offenses: 18 U.S.C. § 922(g) [unlawful possession of a firearm].

4. **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

The property to be searched is a red iPhone [Device] with '(PRODUCT)RED' printed on the back at the bottom in silver color font, the apple logo is silver in color and is placed in the middle of the phone on the rear, which is in the custody of Calhoun County Jail, taken from Diapolis Smith at intake on 14 Aug. 2020.

5. The **Device** is currently located at the Calhoun County Jail, in the Southern Division of the Western District of Michigan.

PROBABLE CAUSE

6. Based on my training and experience, and the facts contained in this continuation, there is probable cause to believe that **Diapolis Tiant Smith**, in the Western District of Michigan, committed the listed crime(s), and that the information described in Attachment B will constitute evidence of these criminal violations.

7. **Smith** is a resident of Battle Creek, Michigan. He is presently in the custody of the U.S. Marshal's Service at the Newaygo County Jail. Smith's criminal history includes a 2007 State of Michigan felony conviction for armed robbery, car-jacking, and conspiracy.

8. During nighttime hours on 14 August 2020, **Smith** was arrested by officers of the Battle Creek Police Department (BCPD) on an outstanding 4-count felony warrant for assault with intent to commit murder related to a domestic assault incident. The arrest was made after BCPD officers saw **Smith** standing in a public street in Battle Creek with numerous other civilians, called out his name, and then pursued him a short distance after he walked away from them and then ran a short distance. When BCPD first encountered him, **Smith** was holding a small red bag (commonly referred to as a "fanny-pack"), which he dropped in the street as officers approached. **Smith** was handcuffed and placed in a BCPD vehicle, and officers retrieved and opened the red bag.

9. The red bag contained a loaded 9mm Jimenez Arms semiautomatic pistol. An ATF

interstate nexus evaluation determined the pistol was manufactured in Nevada, and subsequent testing established that it is a functioning firearm. On 2 March 2020, the gun was reported as having been stolen out of a vehicle to the Riverdale Police Department in Riverdale, Georgia. **Smith** was indicted on 13 Oct. 2020 in this Court's case number 1:20-CR-165 with possessing that pistol as a felon. That case is pending trial.

10. After his arrest, **Smith** was transported to the Calhoun County jail in the BCPD vehicle, and was allowed to keep his cellular telephone during transport. The vehicle was equipped with an audio and visual recording device oriented towards the backseat where **Smith** was sitting, and that **Device** recorded him making a series of phone calls on his cellular telephone to other persons. In these calls, **Smith** told others that he had been arrested, lamented that he was going to prison, and made several references to a "his" red bag, asking these other persons to retrieve it for him.

11. On 26 March 2021, I interviewed Smith's sister. She stated that **Smith** had called her after his arrest, and asked her to contact two of his friends and to retrieve a red bag of his from them that contained a user quantity of marijuana. The sister claimed that she had done as **Smith** asked, and also stated that he told her that police were trying to "plant a gun on him." I have been unable to identify or to contact these two friends of Smith's, or to discover evidence substantiating Smith's sister's story about the red bag.

12. In a public "YouTube" video that was posted on 30 June 2020, **Smith** appears in a rap music video and points what appears to be a cocked Sig Sauer P226 semi-automatic pistol at the camera. That is a different pistol from the weapon recovered on 14 August, but I am advised by the U.S. Attorney's Office that the Government intends to use the video as Rule 404(b) evidence at Smith's trial.

13. The **Device** is currently in the lawful possession of the Calhoun County Jail, where it was inventoried during Smith's booking process. Its condition has not been altered since it was taken from **Smith**. This was the only telephone in **Smith's** possession during his arrest and has been in the custody of Calhoun County Jail since.

14. Because **Smith** possessed and used the **Device** in the interim between his arrest and booking, and used it to communicate with other person's about a red bag, there is probable cause to believe that evidence about the meaning of Smith's references will be found on the **Device**. Also, because the charged pistol was reported stolen in Georgia in March 2020, roughly five months before it was discovered in the red fanny-pack that **Smith** discarded as he attempted to elude BCPD officers, there is probable cause to believe that communications related to Smith's acquisition of the firearm will be found on the **Device**. Finally, there is probable cause to believe that the **Device** will contain one or more communications, and perhaps images, related to the production and publishing of the video and the pistol that **Smith** brandishes in it. If so, this evidence would strengthen the Government's argument for admission of the video at trial.

15. In my training and experience, criminals including illegal gun possessors make extensive use of mobile telephones to facilitate all aspects of their dealings, including making arrangements to acquire guns. Owners of cellphones also routinely keep their mobile telephones in their possession. Those devices leave a cellular location "trail" by their perpetual receipt and transmission of data. Mobile phones often contain evidence indicative of gun trafficking, including records of incoming and outgoing calls and text messages with co-conspirators and suppliers and customers of illegal gun sales ; voicemail messages; photographs of firearms, coconspirators, or currency; and, in the case of "smart phones," Global Positioning System (GPS) data indicating the location of the device at given points in time, providing evidence that the device was in gun

trafficking areas, or evidencing the route used in the theft and trafficking of stolen guns. Further, these types of devices are used to access social media websites such as Facebook, Instagram, etc. In my training and experience, I know that gun traffickers use social media with increasing frequency to communicate with suppliers and purchasers of guns.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated

"GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g.,

121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that the **Device** has capabilities that allow it to serve as **a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA.** In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

22. I respectfully submit that this affidavit supports probable cause for a warrant to search the **Device** described in Attachment A and to seize the items described in Attachment B.